Position Description

Position Description	
JOB ID:	12995
Position Number:	02020960
UC Path Position #	40224568
Dept:	IET - INFORMATION SECURITY OFFICE - 061418
Position:	Senior Information Security Analyst
Approved Payroll Title Code:	0661
Approved Payroll Title:	IT SECURITY ANL 4
Approved MSP Salary Grade:	
Approved PSS Salary Grade:	MSP25
POSITION DETAILS	
Job Summary:	Under the general direction of the Deputy Chief Information Security Officer (DCISO), manage security and data protection solutions that support the University's mission and research, and protect the confidentiality, integrity and availability of information assets owned by or entrusted to UC Davis. This includes ensuring that new and existing information technology (IT) systems meet the University's information assurance (IA) and security requirements, and reviewing and developing information security programs, policies, standards and procedures that enable the campus to address risks and comply with laws and regulations governing data protection. Work with all levels of the University, peers at other UC campuses, and business partners to establish and maintain a strong and adaptive security posture that aligns with organizational risk tolerance, information access requirements, and University strategies. This position also develops and coordinates the Information Security Office's (ISO) awareness and outreach programs to address evolving security threats, maintains a number of security reports and dashboards, participates in technology audit activities, and partners with business and campus units throughout the university community.
Campus Job Scope:	
Department Specific Job Scope:	The Information Security Office (ISO), a division of Information & Educational Technology (IET), helps protect the confidentiality, availability and integrity of UC Davis' information assets through consultation, services and programs. The ISO offers support, assistance, education and advice, manages certain security processes, and helps individuals and departments understand how they are responsible for information security at UC Davis as well as how to meet that responsibility.
Positions Supervised:	
Essential Responsibilities:	50% INFORMATION SECURITY CONSULTING & OUTREACH Outreach & Training: Represent the ISO and its mission, program, products, and services to relevant stakeholders. Develop, manage and lead the ISO's information security awareness/training program. Coordinate the ISO's outreach & training program. Monitor the campus threat environment for emerging threats, and advise relevant stakeholders on the appropriate courses of action. Co-manage the ISO's UC-wide information security symposium.

	Manage 3-4 campus wide campaign's per year. Research & Faculty Support: Provide guidance and assesses client requirements to determine if additional security services are needed; promote good security practices where required. Work with academic and business units to define acceptable levels of residual risk. Review information security requirements in research agreements and contracts Work directly with researchers to review security requirements and ensure understanding of, and compliance with, applicable laws and regulations. 25% POLICY COORDINATION Develop and manage UCD information security policies. Identify where existing policies & procedures require change to reduce risks to campus information assets. Manage UCD's information security exceptions management process. Evaluate and support the documentation, validation, and accreditation processes necessary to assure that new and existing information technology systems meet the University's information assurance and security requirements. Prepare and review system security architecture designs. Draft and review new and existing information security policies, standards and procedures that enable the campus to address information security risks and comply with laws and regulations governing data protection. 20% DOCUMENTATION & REPORTING Prepare new, and maintain existing, security assessment checklists and analysis documentation as required to ensure security assessments are reliable, efficient, and effective. Develop formal assessment reports for management including mitigation recommendations and status. Develop and manage information security metrics program. Develop reports & presentations on the information security program. Provide regular reporting on the current status of the information security program to senior leaders. Prepare/maintain various security reports and dashboards. Participate in technology audit activities. Debrief the Chief Information Security Officer (CISO) on current and emerging issues on information security. 5% OTHER DUTIES Maintain technical currency, including system-wide security policies and initiatives, evolving campus needs, technology capabilities, and threat intelligence from a variety of sources to optimize data protection measures. Other duties and special projects as assigned.
Physical Demands:	

Work Environment:	Adhere to workplace safety practices, read information communicated about workplace safety, complete required safety training on time, report any workplace safety issues promptly to their supervisor or the designated safety coordinator. Work alternate or extended hours on short notice. Occasional travel is required to campus and off campus worksites. Due to the mission-critical services provided by this department, this position may work hours other than M-F 8-5, especially during system development, hardware or software installation, or in response to system problems. UC Davis is a smoke and tobacco free campus. Smoking, the use of smokeless tobacco products, and the use of unregulated nicotine products (e-cigarettes) will be strictly prohibited on any UC Davis owned or leased property, indoors and outdoors, including parking lots and residential space.
Background Check:	Yes
QUALIFICATIONS	
Minimum Qualifications:	Bachelor's degree in computer science or related area or equivalent experience/training. Experience as an information security professional. Experience reviewing, developing and drafting information security policies, standards and new programs. Knowledge of and experience with relevant legal/regulatory security requirements (e.g., FERPA, HIPAA, PCI, & FISMA). Knowledge of and experience working with common information security frameworks, such as ISO/IEC 27001, ITIL, & NIST. Written/verbal communication and interpersonal skills to communicate security and risk-related concepts to technical and non-technical audiences.
Preferred Qualifications for Selection:	Information security professional certification (e.g., CISSP, CISM, CISA, ISA, or other similar credentials). Experience leading information security awareness programs. Experience managing and planning events/campaigns. Experience working with service providers, including contract and vendor negotiations. Experience as information security professional in a higher education setting.

Expectations	
Job Expectations	-Read and follow the UC Davis Principles of Community -Support UCD & IET's mission and values. -Must stay abreast of system-wide security policies and initiatives, evolving campus needs, technology capabilities, and threat intelligence from a variety of sources to optimize data protection measures. -Accountability for the safekeeping of resources in the employee's care and custody and for following and implementing the cyber-safety guidelines. -Excellent organizational and analytical skills. Personal integrity & ability to professionally handle confidential matters -High degree of initiative, dependability & ability to work with little supervision. -Ability to manage multiple projects under strict timelines & work well in a demanding/dynamic environment.

	-Communicate with users in non-technical terms on technical issues. -Communicate on a technical level with other knowledgeable persons. -Excellent skills to establish priorities, organize tasks, and direct effective implementation of tasks in a demanding work environment. -Willingness to learn and apply new technology and willingness to develop skills to promote professional growth. -Willingness to routinely stay in communication with technical staff at other organizations to stay abreast of computing developments and resources available over the network. -Excellent communication (oral, written, presentation, documentation) and interpersonal skills, using tact and diplomacy for interactions with clients and vendors. -Independently follow projects through to successful completion with a high degree of quality. -Experience learning from technical manuals, journals and continuing education and apply that information. -Work in a team environment to provide complex distributed and integrated mission-critical services and to solve technical problems in this environment. -Maintain flexibility in a continuously changing and fast paced work environment. -Make well planned decisions. -Work with a diverse group of people in such a manner as to build high morale and group commitments to goals and objectives. -Work cooperatively with others to achieve and maintain a strong client service environment.